St Hugh of Lincoln RC Primary School

Online Safety Policy

Updated: September 2022 (KCSIE Update)
Review date: September 2023

Any parent/carer/adult with concerns regarding **any aspect of online safety** should report this to the Headteacher (Designated Safeguarding Lead)

1. Introduction

"New technologies inspire children to be creative, communicate and learn. However, while the internet is a great resource, it is important that children and young people are protected from the risks they may encounter." DfE 2015

At St Hugh of Lincoln Primary School we understand the importance of the internet and how new technologies can enhance our children's learning experiences. We also recognise the safety implications of using such technologies and are therefore committed to ensuring that all our children, staff and families recognise how to use the internet and devices in a safe way. The Online Safety policy relates to other policies including those for Computing, Behaviour Management and Anti-Bullying, Safeguarding and Child Protection.

- The school has an Online Safety Coordinator who will attend appropriate training and will provide support and training for all staff and volunteers.
- The school also has a group of older children who are Internet Safety Champions (JOSO'S and have attended training and workshops.
- Our online safety policy has been written by the school, building on guidance from Trafford LA and the Government. It has been agreed by SLT and approved by Governors.
- The online safety policy will be reviewed biannually and with reference to CPOMS (Child Protection Online Monitoring System) where a record will be kept of any inappropriate use of the internet.

2. Use of the Internet

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management of information and administration systems. Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

2.1 How to ensure Internet use will enhance learning

- The school internet access will be designed for pupil and teaching use and will include filtering policies appropriate to the age of our children, provided by Trafford Council to ensure only safe websites can be accessed.

- Pupils will be taught what acceptable internet use is and be given clear objectives on how to do so.

- Pupils will be educated in the effective use of the Internet as a research tool, including the skills of knowledge location, retrieval and evaluation.

2.2 Pupils will be taught how to evaluate internet content

- The school will ensure pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations, acknowledging sources of information used.

- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. For example making pupils aware of the increase in 'Fake news' and websites on the internet and how to use their judgement to identify whether what they are reading is true or false.

3. Managing Internet Access

3.1 Information System Security

- School ICT systems capacity and security will be reviewed regularly.

- Virus protection will be updated regularly.

- The security of the school network relies on the central firewall implemented by Trafford MBC. No traffic shall enter or leave the TMBC Infrastructure without being explicitly permitted by the firewall. No traffic shall route directly between connected establishments unless it has been explicitly allowed to do so.

- Password security is of the utmost importance and must be maintained at all times. Adults and children will be reminded never to disclose their passwords. The abuse of passwords must be reported immediately to the Online safety co-ordinator and recorded on CPOMS.

3.2 Managing filtering

- Developing good practice in internet use as a tool for teaching is essential. School internet access will be designed for pupil and teaching use and will include filtering policies appropriate to the age of the children.

- The school will work with the TMBC, DfE and its internet provider service to ensure systems to protect pupils are reviewed and improved. The filtering solution is currently managed by TMBC to filter the internet stream to the school.

- School iPads and Chrome books are filtered by the same filtering solution as the other internet-connected devices in school so that children cannot access inappropriate content.

- No filtering system is perfect and pupils (and staff) will be taught what to do if they experience material they find distasteful, uncomfortable or threatening. This will be recorded on CPOMS and reported to the Online Safety Co-ordinator. The URL and content will be reported to the ICT Manager who in turn will contact the TMBC ICT service team to have the content blocked. The CPOMS record will be reported to the LADO.

3.3 Social Media platforms

- The school will control access to moderated social networking sites and educate pupils in their safe use.

- Our policy is to block/filter access to other social networking sites such as 'Facebook', 'Twitter', 'Instagram' etc. (Most have a minimum age of 13 specified).

- The school has a Twitter account which is managed by the Headteacher. It is used for sharing general news items and events and personal views are not shared.

- Pupils will be taught the importance of personal safety when using social networking sites, apps and chat rooms through assemblies and designated online safety lessons. They will be advised never to give out personal details of any kind which may identify them or their location. They will be taught never to use a personal images of themselves.

- Pupils will be taught never to meet up with anyone they do not know. Older children will be instructed to always let an adult know if they are leaving the house and when they are likely to return.

- Pupils will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Materials or comments which may be perceived to victimise or bully someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented. Any misuse will be recorded on CPOMS.

- Staff will not exchange personal social networking addresses or use social networking sites to communicate directly with pupils.

3.4 E-mail and other communications systems

- Pupils may only use approved, teacher supervised, e-mail accounts (which do not personally identify them) on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail and this will be recorded on CPOMS.
- Pupils must not reveal personal details about themselves or others in e-mail communication. Arrangements to meet anyone will only be where it is part of a school project and pupils are working under the supervision of their teacher.
- Pupils will be taught about the dangers of computer viruses and how these can be transferred via email attachments.
- Personal e-mail or messaging between staff and pupils should not take place.

3.5 Published content and school website

- Editorial guidance will ensure that the school's ethos is reflected in the website and Twitter page, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material. The Headteacher and Computing Leader will periodically review the content of the school's website and edit as necessary. Class teachers will be responsible for the content on their own Class Blog webpages.
- The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.

3.6 Publishing pupil's images and work

- Photographs that include pupils will be selected carefully and will not be labelled so individual pupils cannot be identified by the general viewing public.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

3.7 Managing videoconferencing and/or direct online communication (SKYPE calls etc.)

- Video conferencing and/or direct online communications is only enabled through the use of Facetime or SKYPE.
- IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Only staff will be enabled to instigate a connection and thus check the suitability of the second party to the call.

- Pupils will be appropriately supervised whilst connected.
- Staff will ensure that the contact details of person(s) communicated with via SKYPE or Facetime are not visible, accessible to or shared with the children at any time.

3.8 Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- When using YouTube staff will vigilantly ensure that;
    - It does not autoplay the next video.
    - They pre-watch the video ahead of time to ensure its content is age-appropriate.
    - They have the video prepared to play before the lesson and will endeavour to ensure that pupils cannot see side-panels or adverts on YouTube.
- Staff should not use mobile phones to take pictures or videos of children they should use their teacher iPad provided by the school. These can be uploaded to the school Twitter account or website.
- Mobile phones are not permitted for use anywhere in school, around the children except in exceptional circumstances. This applies to all members of staff and other visitors to the school.
- Staff should take a mobile phone with them on a school trip/visit outside of school, for use in emergencies only.
- Children who bring mobile phones/tablets to school are required to hand them in to the school staff every morning and devices are collected at home time. It is school policy that only Y6 children may bring in mobile phones.

3.9 Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Any personal data transported out of school on laptops, USB devices or other forms of storage will be encrypted and protected by password protection systems (Sophos).

4 Policy decisions

4.1 Authorising Internet access

- All staff will sign an ‘Acceptable ICT use Agreement’ before using any school ICT resource.

- The school will keep a record of any online safety issue or violations of the user policies. For instance a member of staff may discover unsuitable material that needs reporting or a pupil's access may be withdrawn.

- At key stage one children's experience of the internet will be through adult demonstration and access to websites under the supervision of an adult.

4.2 Assessing risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Our education programme for internet safety with pupils will give them clear strategies and processes for dealing with anything that causes them to feel uncomfortable (Hector's world screen shade).

- The school will audit ICT provision regularly to establish if the –safety policy is adequate and that its implementation is effective.

4.3 The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material or radicalisation when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our Computing curriculum. Our staff are aware of the risks posed by online activity of extremists through training (e.g. Prevent) and have a duty to take action if they believe the well-being of any pupil or adult is being compromised.

5 Communicating the Policy

5.1 Introducing the Online Safety Policy to pupils

- Online safety rules will be posted around school and discussed with the pupils at various points in the school year.

- Pupils and staff will be informed that the network and internet use will be monitored and that misuse will be dealt with appropriately.

- Pupils and Parents will sign an Online Safety Agreement.

- Pupils will be taught appropriate and responsible behaviours for using the internet and communication tools within Computing, RHE and across the curriculum. Misuse will be recorded in the online safety log.

- Pupils will be instructed in responsible and safe use before being allowed access to the internet and will be regularly reminded of the rules and risks.

5.2 Staff and the Online Safety Policy

- All staff will be given the key points of the online safety policy and its importance explained. This will be part of the induction process for any new member of staff.

- Staff are made aware that internet traffic is monitored by TMBC and traced to the individual user. Any potential misuse will be reported to the school and/or the police where appropriate. Discretion and professional conduct is essential.

5.3 Enlisting parents' support

- Parents will be asked to read through the online safety rules with their child. This will be signed by pupil and parent and returned to school.

- Parental attention will be drawn to the school online safety policy in newsletters, the school brochure and on the school Web site.

6 Community use of the internet

- The school's ICT resources may be used by community groups. All adult users will sign an acceptable use policy and will be aware of the school's online safety policy.

7 Handling online safety concerns

- The staff, children and parents/carers will know how and where to report incidents (online safety coordinator, CPOMS and CEOP (Child Exploitation and Online Protection).

- Concerns related to safeguarding issues will be dealt with through the school's Safeguarding Policy and Procedures.

- Complaints of the internet misuse will be dealt with by a senior member of staff in accordance with the schools behaviour policy.

- Any complaint about staff misuse must be referred to the Head teacher.

A new classification of online risk includes the 4Cs

The new CO:RE 4Cs classification recognises that online risks arise when a child:

- engages with and/or is exposed to potentially harmful CONTENT;

- experiences and/or is targeted by potentially harmful CONTACT;
- witnesses, participates in and/or is a victim of potentially harmful CONDUCT;
- is party to and/or exploited by a potentially harmful CONTRACT.

	Content Child as recipient	Contact Child as participant	Conduct Child as actor	Contract Child as consumer
Aggressive	Violent, gory, graphic, racist, hateful and extremist content	Harassment, stalking, hateful behaviour, unwanted surveillance	Bullying, hateful or hostile peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, gambling, blackmail, security risks
Sexual	Pornography (legal and illegal), sexualization of culture, body image norms	Sexual harassment, sexual grooming, generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messages, sexual pressures	Sextortion, trafficking for purposes of sexual exploitation, streaming child sexual abuse
Values	Age-inappropriate user-generated or marketing content, mis/disinformation	Ideological persuasion, radicalization and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, peer pressures	Information filtering, profiling bias, polarisation, persuasive design
Cross-cutting	Privacy and data protection abuses, physical and mental health risks, forms of discrimination			

St Hugh of Lincoln RC Primary School
ICT Acceptable Use Policy: All Adults Working In School

All adults working with ICT equipment at St Hugh of Lincoln School must ensure that they have read, and agree to abide by, the points below.

For personal use:

- Do not give anyone access to your login name or password. Do not use another person's login details.
- Do not open other people's files without express permission. However, the Headteacher may be able to access files of all other staff members in extreme circumstances. Do not corrupt, interfere with or destroy any other user's information.
- Do not release personal details including phone numbers, fax numbers or personal e-mail addresses of any colleague or student over the Internet.
- Do not attempt to visit sites which might be considered inappropriate. All sites visited leave evidence on the computer. Downloading some material is illegal and the police or other authorities may be called to investigate such use.
- Use of school Internet access for business, profit, advertising or political purposes is strictly forbidden.
- The Internet should not be used for personal reasons during working hours.
- Users should close their browser and log out when their session has finished.
- No files on school ICT equipment can be considered private.
- The school can in no way be held responsible for loss of personal information from the network.
- The above points also relate to work off site using school ICT equipment.
- School Ipads remain the property of school and should be used appropriately. A breach in acceptable use would result in their withdrawal. Damages must be paid for if a result of unacceptable use.
- School related content should not be put on social media and staff should not comment on any school related issues on such platforms, unless it is officially communication on the school Twitter account (managed by M Mountcastle and A Smith)
- Photographs are often taken for display and assessment purposes on school cameras/Ipads which are printed or saved on school computers.
- Images should not be taken on personal mobile devices.
- Mobile phones must be on silent during lesson times and not used for personal calls, sending or reading texts during these times.

Personal E-mail

- Observe *netiquette* on all occasions. E-mail should not be considered a private medium of communication and could be subject to monitoring both internally and externally.
- Do not include offensive or abusive language in your messages or any language which could be considered defamatory, obscene, menacing or illegal. Do not use language that could be calculated to incite hatred against any ethnic, religious or other minority.
- Make sure nothing in the messages could be interpreted as libellous.
- Do not send any message which is likely to cause annoyance, inconvenience or needless anxiety.
- Do not send any unsolicited promotional or advertising material nor any chain letters or pyramid selling schemes.

When using the Internet or e-mail with students

- Remind students of the rules for using the Internet and e-mail.
- Watch for accidental access to inappropriate materials and report the offending site to Miss Moran/Mr Mountcastle.
- Check before publishing student's work; make sure that you have parental permission.

Please sign below and copy. Keep one copy for your records and return the other to Mr Mountcastle

I have read and agree to abide by the Acceptable Use Policy of St Hugh of Lincoln School.

Name:
Job/Position:
Signature:
Date:

Online Safety Agreement

Both pupils and their parents/carers are asked to sign to show that the Online Safety Rules on the reverse of this agreement have been understood and agreed.

Consent for internet access and related technologies

I have read and understood the school's Online Safety Rules and give permission for my child to access the internet and e-mail and message accounts as part of the school curriculum. I understand that the school:

- ✔ Will take all reasonable precautions to ensure that pupils cannot access inappropriate materials but I appreciate that this is a difficult task.
- ✔ Cannot be held responsible for the content of the materials accessed through the internet. I agree that the school is not liable for any damages arising from use of the internet facilities.
- ✔ May use monitoring software where this is available to ensure that inappropriate materials are not being stored or used on school equipment.

I understand that if my child fails to follow the Online Safety Rules that this may result in them not being permitted to use computers, the Internet and other new technologies in school. Furthermore, I understand that when using social networking sites, the school may take legal action if I mention the school or individual pupils in a negative or derogatory way.

Please print name_____

Signed by Parent/Carer _____ Date_____

Consent for Web publication of work and photographs

I agree that images of my child and their work may be published on the school Website and other related material to promote the school which may sometimes include use by this and other educational authorities.

Photographs will always show your child in a positive role and will not include their full name.

Signed by Parent/Carer:_____ Date:_____

Online Safety Rules

Think then click

We use computers, the internet and lots of other new technologies to help us learn. To keep us safe when using them we must:

- ✔ Ask permission before using the internet.
- ✔ Only use websites that an adult has chosen.
- ✔ Immediately minimise or switch off the screen for any website we are unsure or uncomfortable about.
- ✔ Tell an adult if we see anything we are uncomfortable with.
- ✔ Only e-mail and message people an adult has approved.
- ✔ Only send emails and messages that are polite and friendly.
- ✔ Do not open e-mails that are sent by anyone we do not know.
- ✔ Never give out personal information of passwords.
- ✔ Never arrange to meet anyone we do not know.
- ✔ Do not use internet chat rooms or social networking sites.

Pupil's agreement

- ✔ I have read and I understand the Online safety rules.
- ✔ I will use the computer, network, internet access and other new technologies in a responsible way at all times.
- ✔ I know that network and internet access can be monitored.
- ✔ If I fail to follow these rules, then I may not be allowed to use the computer, network, internet or other new technologies in school.

Pupil name:_____ Class:_____

Signed by pupil_____ Date:_____